

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
WACO DIVISION**

<b>CYBERSOFT IP, LLC</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	<b>Civil Action No. 6:21-cv-00157</b>
<b>v.</b>	)	
	)	
<b>BLACKBERRY CORPORATION</b>	)	<b>JURY TRIAL DEMANDED</b>
<b>Defendant.</b>	)	

**PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT  
INFRINGEMENT**

Cybersoft IP, LLC (“Cybersoft”) files this Original Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent No. 6,763,467 (“the ‘467 patent”) (referred to as the “Patent-in-Suit”) by Blackberry Corporation (“Blackberry”).

**I. THE PARTIES**

1. Plaintiff Cybersoft is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, Blackberry is a corporation existing under the laws of the State of Texas, with a principal place of business located at 11501 Alterra Parkway, Suite 410, Domain Seven, Austin, Texas 78758. On information and belief, Blackberry sells and offers to sell products and services throughout Texas, including in this judicial district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that

they would be sold in Texas and this judicial district. Blackberry may be served through their registered agent Corporate Creations Network, Inc., 5444 Westheimer #1000, Houston, TX 77056.

## **II. JURISDICTION AND VENUE**

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to patents, namely, 35 U.S.C. § 271, et. seq.

4. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

5. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

## **III. INFRINGEMENT**

### **A. Infringement of the '467 Patent**

6. On July 13, 2004, U.S. Patent No. 6,763,467 (“the ‘467 patent”, attached as Exhibit A) entitled “Network Traffic Intercepting Method and System” was duly and legally issued by the U.S. Patent and Trademark Office. Cybersoft owns the ‘467 patent by assignment.

7. The ‘467 patent relates to a novel and improved method and system for protecting computers from invasion by viruses, trojan horses, worms, and other malicious algorithms.

8. Blackberry maintains, operates, and administers online and software based training platforms, products and services that facilitate remote training that infringes claim 1 of the ‘467 patent, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the ‘467 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

9. Support for the allegations of infringement may be found in the following preliminary table:

<p>1. A method conducted within a single computer system connected to a network for intercepting, examining, and controlling data flowing via transport connections between the transport layer of an operating system and user applications, said method comprising the steps of:</p>	<p><b>“The BlackBerry Cyber Suite is a comprehensive unified endpoint security (UES) solution.</b> It provides complete prevent, detect, and respond cybersecurity to enterprises of any size in any industry... <b>The BlackBerry® Cyber Suite provides complete security, effectively preventing breaches and safeguarding against sophisticated threats</b> with advanced AI. It provides a total Zero Trust solution with <b>coverage across the full spectrum of devices, ownership models, network, apps and people.</b> It continuously authenticates users and <b>dynamically adapts security policies</b> to deliver a Zero Touch experience that improves security with no user interruption.” [1]</p> <p>“BlackBerry Spark UES Suite offers the broadest set of security capabilities and visibility through six interconnected technologies, or pillars. These pillars work in tandem to calculate risk, share data, and enable better policy controls...</p> <p>1. <b>Endpoint Protection[:]</b> <b>Automated malware prevention</b> powered by AI, combined with <b>application and script control</b>, memory protection, and <b>device policy enforcement</b> to predict and prevent cyber attacks</p> <p>2. <b>Endpoint Detection and Response (EDR)[:]</b> AI-based, prevention-first <b>endpoint detection and response stops attacks before they can execute</b>, and <b>automates investigation and response</b> with playbook-based workflows</p> <p>3. <b>Mobile Threat Defense (MTD)[:]</b> Leverages AI to <b>monitor mobile devices and the apps running on them</b> for any new or known threats (<b>including malicious URLs and phishing</b>) and takes appropriate action to remediate...</p> <p>6. <b>Secure Web Gateway*[:]</b> Provides several capabilities to meet the Zero Touch objective of instant, secure, and VPNless mobile access on any device: • <b>Continuous and contextual authentication</b> • <b>Traffic segmentation</b> • <b>Threat prevention</b> • <b>Reporting and analysis</b>” [2]</p> <p>“<b>BlackBerry Protect</b>, which provides the foundation for <b>BlackBerry Optics</b>, is designed to specifically prevent successful attacks aimed at endpoints. This includes:</p> <ul style="list-style-type: none"> <li>• <b>Identifying and blocking malicious executable and file identification</b> using AI</li> <li>• <b>Controlling where, how, and who can execute scripts</b></li> <li>• Managing the use of USB devices, prohibiting unauthorized devices</li> <li>• Eliminating the ability for attackers to use fileless malware attack techniques</li> <li>• <b>Preventing malicious email attachments from detonating</b> their payloads” [3] <p>“BlackBerry Optics is an EDR solution that extends the threat prevention delivered by BlackBerry Protect using AI to identify and prevent widespread security incidents. BlackBerry Optics provides:</p> <ul style="list-style-type: none"> <li>• <b>AI-driven incident prevention</b></li> <li>• <b>Context-driven threat detection</b></li> </ul> </li></ul>
--	--

	<ul style="list-style-type: none"> <li>• Machine learning <b>threat identification...</b></li> <li>• <b>Automated remote investigations</b></li> <li>• <b>Dynamic playbook-driven response capabilities</b>" [3]</li> </ul> <p>"Configuring <b>TLS/SSL connections...</b></p> <p>1. On the menu bar, clicks Settings &gt; External Integration &gt; BlackBerry Secure Gateway...</p> <p>3. <b>Click the TLS version or cipher that you want to add or remove from the Selected list...Click Assign</b>" [4] p. 36-37</p>
a) intercepting all said data flowing between said transport layer and said user application;	<p>"<b>Endpoint Detection and Response (EDR)</b>[:] AI-based, <b>prevention-first and point detection and response stops attacks before they can execute</b>, and automates investigation and response with playbook-based workflows" [2]</p> <p>"The agent will <b>scan and monitor running processes to protect devices from malware</b> that attempts to take advantage of software vulnerabilities that exploit running processes or executes from within memory space. It is recommended that you block all types of memory violations." [5] p.12</p> <p>"CylancePROTECT also offers Memory Protection and <b>script control</b> as optional protective policy components. Running the CylancePROTECT agent at the guest OS level on each virtual machine provides the added benefit of being able to protect against malicious scripts and malicious processes running in memory...Both of these functions <b>use a process injection method whereby the agent code injects itself into running processes to identify and block unwanted or unauthorized code</b> from running." [5] p.106</p> <p>"<b>Script control monitors and protects</b> against scripts running in your environment. <b>The agent is able to detect the script and script path before the script is executed.</b> Depending on the policy set for script control (alert or block), the agent will allow or block the execution of the script." [5] p.24</p> <p>"Users can quickly search for <b>files, executables, hash values, and other IOCs</b> across the <b>entirety of their network endpoints</b> to uncover hidden threats." [3]</p>
b) examining said data for information content, which comprises examining said data streams to determine if they are scannable for information content or nonscannabl	<p>"<b>Endpoint Threat Detection: Suspicious behaviors and other indicators of potential compromise on endpoints will be uncovered</b> automatically." [3]</p> <p>"The BlackBerry Protect architecture consists of a lightweight single agent that is managed via BlackBerry's own SaaS-based cloud console... <b>The endpoint agent will detect and prevent malware</b> on the host, independent of a cloud connection and without the need for continuous updates. BlackBerry Protect is capable of detecting and quarantining malware in open, isolated, and virtual networks." [6]</p> <p>"The agent will <b>scan and monitor running processes to protect devices from malware</b> that attempts to take advantage of software vulnerabilities that exploit running processes or executes from within memory space." [5] p.12</p> <p>"CylancePROTECT can do more than simply <b>classify files as unsafe or abnormal. It can provide details</b> on the static and dynamic characteristics of files." [5] p.47</p>

<p>e for information content; passing said nonscannable data streams to said user application; and passing said scannable data streams to said processing step (c) wherein said information content includes the presence of proscribed data; and,</p>	<p>“The Cylance score represents the confidence level that the file poses a real <b>danger to your environment</b>. The higher the score, the greater the confidence level that the file can be used for malicious purposes. <b>Based on the score, threats are considered either unsafe or abnormal...</b>The Cylance score is <b>independent of threat classification</b>.” [5] p.47-48</p> <div data-bbox="415 415 1409 577" style="border: 1px solid black; padding: 5px;"> <p><b>Unsafe and abnormal files</b></p> <p><b>Unsafe:</b> A file with a score ranging from 60-100. An unsafe file is one that the CylanceINFINITY finds attributes that greatly resemble malware.</p> <p><b>Abnormal:</b> A file with a score ranging from 1-59. An abnormal file has a few malware attributes but less than an unsafe file, thus is less likely to be malware.</p> </div> <p style="text-align: right;">[5] p.47</p> <div data-bbox="509 625 1312 764" style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> <li>• <b>Unsafe:</b> The file is classified as unsafe, but no action has been taken.</li> <li>• <b>Quarantined:</b> The file was already quarantined due to a policy setting.</li> <li>• <b>Waived:</b> The file was waived or safe listed by the administrator.</li> <li>• <b>Abnormal:</b> The file is classified as abnormal, but no action has been taken.</li> </ul> </div> <p style="text-align: right;">[5] p.53</p> <p>“The CylanceOPTICS Detections feature is powered by the <b>Context Analysis Engine (CAE)</b> - a highly performant and optimized engine that statefully <b>analyzes and correlates events as they occur on an endpoint in near real time...</b> To complement the capabilities of the CAE, CylanceOPTICS can take <b>automated response actions against Artifacts of Interest (AOI) identified by the CAE</b>. These Response Actions, again, are stored locally on the endpoint, <b>allowing CylanceOPTICS to function as another layer of prevention in addition to CylancePROTECT.</b>” [7] p.45</p>
<p>c) processing said data, including scanning said data for said proscribed data, based on said information content to protect the computer system and the network by preventing said computer system and</p>	<p>“The CylanceOPTICS Detections feature is powered by the <b>Context Analysis Engine (CAE)</b> - a highly performant and optimized engine that statefully <b>analyzes and correlates events as they occur on an endpoint in near real time</b>. The CAE stores its logic locally on the endpoint, allowing it to monitor and track malicious or suspicious activities on an endpoint even when no connection to Cylance's cloud services is available...To complement the capabilities of the CAE, CylanceOPTICS can take automated response actions against Artifacts of Interest (AOI) identified by the CAE. These Response Actions, again, are stored locally on the endpoint, <b>allowing CylanceOPTICS to function as another layer of prevention in addition to CylancePROTECT</b>” [7] p.45</p> <p>“The flexibility of the CAE lets you utilize the <b>logic to monitor for broad behavior characteristics</b> (such as files being created with <b>certain naming patterns</b>) or search for a <b>targeted series of events</b> (such as a <b>process with a certain file signature thumbprint</b> that then creates files and initiates network connections). These custom rules operate in the same workflows as rules provided by Cylance and can have the same automated response actions to stop <b>malicious activities</b> from occurring the moment <b>CylanceOPTICS identifies them.</b>” [7] p.49</p>

<p>network from accessing proscribed data,</p>	<p><b>“Once a hash has been quarantined (either through local or global quarantine), the agent will continue to prevent that file from executing on that device.</b> If the file name is changed or the file is copied to a new location on the device, the agent will continue to perform the same actions.” [5] p.12</p> <div data-bbox="412 415 1427 863"> <p><b>Threat indicator categories</b></p> <p>Each category represents an area that has been frequently seen in malicious software and is based on deep analysis of over 100 million binaries. The threat indicators report indicates how many of those categories were present in the file.</p> <ul style="list-style-type: none"> <li>• <b>Anomalies (20 indicators)</b> – The file has elements that are inconsistent or anomalous in some way. Frequently, they are inconsistencies in the structure of the file.</li> <li>• <b>Collection (21 indicators)</b> – The file has evidence of data collection. This can include enumeration of device configuration or collection of sensitive information.</li> <li>• <b>Data Loss (12 indicators)</b> – The file has evidence of data exfiltration. This can include outgoing network connections, evidence of acting as a browser, or other network communications.</li> <li>• <b>Deception (22 indicators)</b> – The file has evidence of attempts to deceive. Deception can be in the form of hidden sections, inclusion of code to avoid detection, or indications of improper labeling in metadata or other sections.</li> <li>• <b>Destruction (13 indicators)</b> – The file has evidence of destructive capabilities. Destruction includes the ability to delete device resources such as files and directories.</li> <li>• <b>Miscellaneous (8 indicators)</b> – These are other indicators that do not fit into other categories.</li> </ul> </div> <p>[5] p.54</p> <div data-bbox="412 905 1427 1209"> <table border="1"> <tr> <td>Auto Quarantine with Execution Control</td><td> <p>This feature quarantines or blocks the unsafe or abnormal file to prevent it from executing. Quarantining a file:</p> <ul style="list-style-type: none"> <li>• Renames the file with a .quarantine extension</li> <li>• Moves the file from its original location to one of the following quarantine directories: <ul style="list-style-type: none"> <li>• <b>For Windows:</b> C:\ProgramData\Cylance\Desktop\q</li> <li>• <b>For macOS:</b> /Library/Application Support/Cylance/Desktop/q</li> <li>• <b>For Linux:</b> /opt/cylance/desktop/q</li> </ul> </li> <li>• The Access Control List (ACL) for the file is modified to prevent the file from being interacted with by the user.</li> </ul> </td></tr> </table> </div> <p>[5] p.10</p>	Auto Quarantine with Execution Control	<p>This feature quarantines or blocks the unsafe or abnormal file to prevent it from executing. Quarantining a file:</p> <ul style="list-style-type: none"> <li>• Renames the file with a .quarantine extension</li> <li>• Moves the file from its original location to one of the following quarantine directories: <ul style="list-style-type: none"> <li>• <b>For Windows:</b> C:\ProgramData\Cylance\Desktop\q</li> <li>• <b>For macOS:</b> /Library/Application Support/Cylance/Desktop/q</li> <li>• <b>For Linux:</b> /opt/cylance/desktop/q</li> </ul> </li> <li>• The Access Control List (ACL) for the file is modified to prevent the file from being interacted with by the user.</li> </ul>
Auto Quarantine with Execution Control	<p>This feature quarantines or blocks the unsafe or abnormal file to prevent it from executing. Quarantining a file:</p> <ul style="list-style-type: none"> <li>• Renames the file with a .quarantine extension</li> <li>• Moves the file from its original location to one of the following quarantine directories: <ul style="list-style-type: none"> <li>• <b>For Windows:</b> C:\ProgramData\Cylance\Desktop\q</li> <li>• <b>For macOS:</b> /Library/Application Support/Cylance/Desktop/q</li> <li>• <b>For Linux:</b> /opt/cylance/desktop/q</li> </ul> </li> <li>• The Access Control List (ACL) for the file is modified to prevent the file from being interacted with by the user.</li> </ul>		
<p>c1) wherein said operating system includes protocols implemented on top of said transport layer, said protocols having a plurality of states, and wherein said processing</p>	<p><b>“IMAP/POP3 email profiles to specify how iOS, macOS, Android, and Windows devices connect to IMAP or POP3 mail servers and synchronize email messages.</b> The required profile settings vary for each device type and depend on the settings that you select.” [4] p.44</p> <p><b>“Protocol[:]</b> This must match what you have configured on your syslog server...<b>TLS/SSL[:]</b> Only available if the protocol specified is TCP, <b>TLS/SSL ensures the syslog message is encrypted in transit from CylancePROTECT to the syslog server.</b> We encourage customers to checkmark this option. Be sure your syslog server is configured to listen for TLS/SSL messages.” [5] p.77</p>		



step further includes the step of parsing, said parsing tracking the state of said protocols with a parser.	(b)
---	-----

Referenc es	
1	<a href="https://www.blackberry.com/us/en/products/blackberry-cyber-suite">https://www.blackberry.com/us/en/products/blackberry-cyber-suite</a>
2	<a href="https://www.blackberry.com/us/en/products/blackberry-cyber-suite">https://www.blackberry.com/us/en/products/blackberry-cyber-suite</a>
3	<a href="https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/ds-bb-optics.pdf">https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/ds-bb-optics.pdf</a>
4	<a href="https://docs.blackberry.com/content/dam/docs-blackberry-com/release-pdfs/en/blackberry-uem/12_13/administration/Email-calendar-contacts-BlackBerry-UEM-12.13-en.pdf">https://docs.blackberry.com/content/dam/docs-blackberry-com/release-pdfs/en/blackberry-uem/12_13/administration/Email-calendar-contacts-BlackBerry-UEM-12.13-en.pdf</a>
5	<a href="https://docs.blackberry.com/content/dam/docs-blackberry-com/releasepdfs/en/cylanceprotect/latest/BlackBerry%20Protect%20Desktop%20Administration%20Guide.pdf">https://docs.blackberry.com/content/dam/docs-blackberry-com/releasepdfs/en/cylanceprotect/latest/BlackBerry%20Protect%20Desktop%20Administration%20Guide.pdf</a>
6	<a href="https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/ds-bb-protect.pdf">https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/ds-bb-protect.pdf</a>
7	<a href="https://docs.blackberry.com/content/dam/docs-blackberry-com/release-pdfs/en/blackberry-optics/2-5/CylanceOPTICS-Admin-Guide.pdf">https://docs.blackberry.com/content/dam/docs-blackberry-com/release-pdfs/en/blackberry-optics/2-5/CylanceOPTICS-Admin-Guide.pdf</a>

These allegations of infringement are preliminary and are therefore subject to change.

10. Blackberry has and continues to induce infringement. Blackberry has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., payment products and services



that facilitate purchases from a vendor using a bridge computer) such as to cause infringement of claim 1 of the '467 patent, literally or under the doctrine of equivalents. Moreover, Blackberry has known or should have known of the '467 patent and the technology underlying it from at least the date of issuance of the patent.

11. Blackberry has and continues to contributorily infringe. Blackberry has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., payment products and services that facilitate purchases from a vendor using a bridge computer) and related services such as to cause infringement of claim 1 of the '467 patent, literally or under the doctrine of equivalents. Moreover, Blackberry has known or should have known of the '467 patent and the technology underlying it from at least the date of issuance of the patent.

12. Blackberry has caused and will continue to cause CYBERSOFT damage by direct and indirect infringement of (including inducing infringement of) the claims of the '467 patent.

#### **IV. JURY DEMAND**

CYBERSOFT hereby requests a trial by jury on issues so triable by right.

#### **V. PRAYER FOR RELIEF**

WHEREFORE, CYBERSOFT prays for relief as follows:

- a. enter judgment that Defendant has infringed the claims of the '467 patent through Blackberry payment links;
- b. award CYBERSOFT damages in an amount sufficient to compensate it for Defendant's infringement of the '467 patent in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;

- c. award CYBERSOFT an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;
- d. declare this case to be “exceptional” under 35 U.S.C. § 285 and award CYBERSOFT its attorneys’ fees, expenses, and costs incurred in this action;
- e. declare Defendant’s infringement to be willful and treble the damages, including attorneys’ fees, expenses, and costs incurred in this action and an increase in the damage award pursuant to 35 U.S.C. § 284;
- f. a decree addressing future infringement that either (i) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patents-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and
- g. award CYBERSOFT such other and further relief as this Court deems just and proper.

Respectfully submitted,

**Ramey & Schwaller, LLP**

A handwritten signature in blue ink, appearing to read 'WPR', enclosed within a large, loopy oval shape.

---

William P. Ramey, III  
Texas State Bar No. 24027643  
5020 Montrose Blvd., Suite 800  
Houston, Texas 77006  
(713) 426-3923 (telephone)  
(832) 900-4941 (fax)  
[wramey@rameyfirm.com](mailto:wramey@rameyfirm.com)

Jeffrey Kubiak (Pro Hac Pending)  
Texas State Bar No. 24028470  
5020 Montrose Blvd., Suite 800  
Houston, Texas 77006  
(713) 426-3923 (telephone)  
(832) 900-4941 (fax)  
[jkubiak@rameyfirm.com](mailto:jkubiak@rameyfirm.com)

***Attorneys for Cybersoft IP, Inc.***